



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Application of :

BAR et al.

Serial No. : 10/774,169

: Group Art Unit: 2155

Filed : February 5, 2004

: Examiner: Thuong Nguyen

For : DETECTING AND PROTECTING AGAINST WORM TRAFFIC ON A
NETWORK

PRE-APPEAL BRIEF REQUEST FOR REVIEW

I. Introductory Comments

Claims 1, 4-26, 28-35, 38-60, 62-69, 72-94 and 96-108 are pending in this application.

Claims 1, 25, 29, 32, 35, 59, 63, 66, 69, 93, 97 and 100 are independent claims.

In an Official Action dated October 11, 2006, all the pending claims were finally rejected. Independent claims 1, 35 and 69 were rejected under 35 U.S.C. 112, second paragraph, for being indefinite. Claims 1, 4-11, 21, 22, 25, 26, 28-35, 38-45, 55, 56, 59, 60, 62-69, 72-79, 89, 90, 93, 94, 96-103, 105 and 107 were rejected under 35 U.S.C. 102(e) over Lyle (U.S. Patent 6,886,102). Dependent claims 12-20, 23, 24, 46-54, 57, 58, 80-88, 91, 92, 104, 106 and 108 were rejected under 35 U.S.C. 103(a) over Lyle in view of other references. In a response filed December 7, 2006, Appellant submitted further arguments as to the patentability of the claims over the cited art. In an Advisory Action dated January 8, 2007, however, the Examiner maintained the rejection of all the claims.

Appellant respectfully submits that Lyle fails to teach, or even to suggest, every element of the independent claims in this application, and furthermore that all the claims in the application are clear and definite. Accordingly, Appellant requests that the application be allowed on the existing claims or, in the alternative, that prosecution on the merits of the claims be reopened with a non-final Official Action.

II. Rejection of independent claims 1, 35 and 69 under 35 U.S.C. 112, second paragraph

In the response of December 7, Appellant pointed out the flaws in the Examiner's grounds of rejection and argued that claims 1, 35 and 69 meet the requirements of 35 U.S.C. 112. In the Advisory Action, the Examiner did not relate to this rejection or to Appellant's arguments in this regard. Appellant believes that the Examiner may have intended to withdraw the rejection under 35 U.S.C. 112. If not, Appellant asks that the Board refer to the

detailed arguments presented in the response of December 7, and reverse the rejection on this basis.

III. Rejection of independent claims 1, 35 and 69 under 35 U.S.C. 102(e) over Lyle

These claims recite a method, apparatus and software product for processing communication traffic that is directed to a group of addresses on a network, based on monitoring traffic that is directed to a subset of the group. The subset of the group of the addresses that is to be monitored is identified such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group. As pointed out in the response of December 7, Lyle neither teaches nor suggests any particular criterion for selection of ports or addresses to be monitored, let alone the specific (and surprising) criterion recited in claims 1, 35 and 69.

In the Advisory Action, the Examiner stated (item 2) that Appellant had argued that “Lyle neither teach nor suggest monitoring the communication traffic that is directed to the addresses in the subset.” This statement is simply incorrect. Appellant made no such argument in the response of December 7. Therefore, this argument is moot.

The Examiner went on to maintain (item 3 in the Advisory Action) that “Lyle does teach identifying or choosing to monitor addresses that are expected to receive smaller amounts of communication traffic,” citing Lyle’s Fig. 8 and col. 14, line 56 – col. 15, line 30. In this passage, Lyle describes how his analysis framework determines whether the number of events associated with a network or sub-network “exceeds a baseline incident rate by a prescribed amount” (col. 14, lines 59-62). It has nothing to do with identifying or choosing to monitor addresses that are expected to receive smaller amounts of communication traffic, as recited in claims 1, 35 and 69. The Examiner has failed to point out even a hint of motivation in Lyle for monitoring low-traffic addresses.

Therefore, independent claims 1, 35 and 69 are patentable over Lyle.

IV. Rejection of independent claims 25, 59 and 94 under 35 U.S.C. 102(e) over Lyle

These claims recite a method, apparatus and software product for processing communication traffic in which traffic originating from a group of addresses is monitored in order to detect a pattern that is indicative of a malicious program running on a computer at one (or more) of the addresses. The pattern is detected by determining that the computer has transmitted packets to a large number of different destination addresses. As pointed out in the

response of December 7, Lyle neither teaches nor suggests applying this sort of detection criterion.

In the Advisory Action (item 4), the Examiner maintained that Lyle teaches this feature in col. 10, lines 19-60, and col. 13, lines 9-21 and 38-55. The passage in col. 10 refers to detection of certain strings, clues, or signatures, as well as detection of a high number of data packets of some type and/or “with a certain target destination or recipient address” (lines 48-49, emphasis added). By contrast, claims 25, 59 and 94 recite the opposite criterion: packets directed to many different destination addresses. The cited passages in Lyle’s col. 13 relate to the manner in which events are handled in order to prevent multiple messages to one destination from masking another message to a different destination (lines 16-18) and to determine whether multiple events should be aggregated into an “existing incident” (lines 37-38). These are internal function of Lyle’s system, which have nothing to do with determining the number of different destination addresses to which a suspect computer has transmitted packets, let alone using the large number of different destination addresses as a pattern indicative of a malicious program running on the computer, as recited in claims 25, 59 and 94.

The Examiner continued this line of misinterpretation of the claim limitations by stating that “Lyle also discloses that the method of detected the router ports if a particular ports is receiving an unusually high number of data packets of any type with a certain target destination or recipient address” (emphasis added). Claims 25, 59 and 94 refer to packets sent to many different destination addresses, and certainly not many packets sent to the same destination address, as the Examiner appears to have interpreted the claim. The Examiner’s next comment that “Lyle discloses the method of determined if the rate of certain types of messages exceeds a normal level” is equally *non sequitur*.

Thus, independent claims 25, 59 and 94 are patentable over Lyle.

V. Rejection of independent claims 29, 63 and 97 under 35 U.S.C. 102(e) over Lyle

These claims recite a method, apparatus and software product in which communication traffic is monitored so as to detect packets indicative of a network communication failure that is characteristic of a worm infection. Upon detecting an increase in the rate of arrival of these packets, the communication traffic is filtered so as to remove at least a portion of the communication traffic that is generated by the worm infection. As

pointed out in the response of December 7, Lyle neither teaches nor suggests applying this sort of detection criterion.

In the Advisory Action, the Examiner stated (item 5) that Appellant had argued that “Lyle neither teach nor suggest filtering the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection.” This assertion is simply incorrect. Appellant made no such statement in the response of December 7. Therefore, this argument is moot.

The Examiner went on to maintain (item 6 in the Advisory Action) that Lyle teaches “detecting an increase in a rate of arrival of the packets that are indicative of the communication failure” in col. 10, line 19 – col. 11, line 1. This passage, however, relates only to detecting the “level or rate” of “certain types of messages” (lines 55-56), without specifying the types of messages that are involved. Lyle makes no mention or suggestion of communication failures or how they should be handled, and does not even hint that packets indicative of such failures could be used in filtering worm-generated traffic as required by the present claims.

Therefore, independent claims 29, 63 and 97 are patentable over Lyle.

V. Rejection of independent claims 32, 66 and 100 under 35 U.S.C. 102(e) over Lyle

These claims recite a method, apparatus and software product in which communication traffic on a network is monitored so as to detect ill-formed packets. The ill-formed packets are used in determining that at least a portion of the traffic has been generated by a worm infection. As pointed out in the response of December 7, Lyle fails to relate in any way to whether packets are well formed or ill formed, and certainly does not suggest that detection of ill-formed packets might be used in determining that a worm infection has occurred.

In the Advisory Action, the Examiner stated (item 9) that “Lyle does teach detecting ill-form packets” in col. 7, lines 9-19. This passage, however, says only that “the sniffers search for data indicating an actual or suspected attack... as described more fully below.” Lyle goes on to describe a number of ways in which the sniffers may search for such attack-related data (see, for example, col. 10, lines 30-59). None of these ways has anything to do with ill-formation of packets.

The Examiner went on to state that “Inherently, Lyle includes the ill-form packets in the suspicious packets,” but this assertion is without support either in Lyle or in the prior art

as a whole. Ill-formed packets may be indicative of a worm attack, as discovered by the inventors in the present patent application, but this does not mean that worm-infected packets are necessarily ill formed. To support her position that Lyle anticipates claims 32, 66 and 100 inherently, the Examiner would have had to provide evidence that "the missing descriptive matter is necessarily present in the thing described in the reference" (*Continental Can Co. USA v. Monsanto Co.*, 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749 (Fed. Cir. 1991), cited in MPEP 2131.01(III)). The Examiner has provided no evidence at all. Lyle mentions many possible signs that could be used to detect worm attacks, but he does not even hint that ill-formation of packets could be one of them.

Therefore, independent claims 32, 66 and 100 are patentable over Lyle.

VII. Rejection of the dependent claims

In view of the patentability of all the independent claims, as explained above, the dependent claims in this application are believed to be patentable, as well. Furthermore, notwithstanding the patentability of the independent claims, Appellant believes that the dependent claims recite independently-patentable subject matter. In the interest of brevity, however, Appellant will defer further argument regarding the dependent claims to the Appeal Brief, in the event that this application proceeds to appeal. For this reason, Appellant has also refrained from addressing item 7 in the Advisory Action, which relates to the limitations of dependent claim 30.

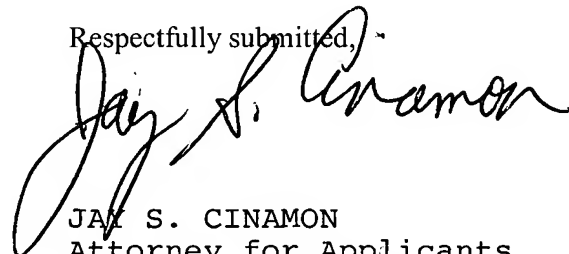
VIII. Conclusion

In view of the above remarks, Appellant respectfully submits that all of the claims in the present application are in order for allowance. Notice to this effect is hereby requested.

Dated: April 11, 2007

ABELMAN, FRAYNE & SCHWAB
666 Third Avenue, 10th Floor
New York, New York 10017-5621
Tele: (212) 949-9022
Fax: (212) 949-9190

Respectfully submitted,


JAY S. CINAMON
Attorney for Applicants
Reg. No. 24,156